Informationsrisker

Informationsriskerna har länge underskattats och hanteringen har ännu inte alltid nått en acceptabel nivå. Ett företag kan i stor utsträckning hantera informationsriskerna självt, men för att skydda exempelvis datanätet krävs ofta sakkunnighjälp. Det viktigaste är att vara medveten om den centrala information som finns i företaget, att utveckla en säkerhetsorienterad verksamhet och att tillämpa säkerhetssystem. Ett tekniskt skydd är endast ett av de element som finns till buds.

Information är en viktig produktionsfaktor

Varje företag besitter information som har stor betydelse för verksamheten, t.ex. kunddata, data om produktionsstyrningen, produktidéer, marknadsföringsplaner. **Informationen är omfattande och finns i många olika former**: det kan vara fråga om personligt kunnande och erfarenhetsbaserade färdigheter; dokument, avtal, instruktioner, planer och övriga pappersdokument samt kund-, order- och lönedata och annan information som finns i företagets datasystem.

För många sm-företag är **informationen det största kapitalet**. Ändå fäster man inte tillräcklig uppmärksamhet på hanteringen och skyddet av denna information. Med tanke på företagets verksamhet är det viktigt att

- Informationen är korrekt, tillförlitlig och up-to-date
- Informationen alltid är tillgänglig för de rätta personerna
- Informationen inte hamnar i orätta händer.

Information innebär besvär - informationsförluster och –läckage medför ännu större besvär!

Informationsriskernas karaktär förändras

Informationsriskernas karaktär ändras ständigt. Företag i alla branscher sysslar i allt högre grad med informationsbehandling – dokument och data överförs och behandlas hela tiden på ett allt mer komplicerat sätt och i allt mer omfattande nät

- Informationen överförs på nytt sätt i företagsnäten
- Arbetsförhållanden förkortas – minskar personalens engagemang?
- Makrovirus är ett nytt hot mot textdokument
- Invandrares uppfattningar eller praxis i ett nytt exportland kan skilja sig från det företaget vant sig vid
- Dataöverföringsalternativen blir fler och snabbare
- Var talar du i din mobiltelefon?
- Internet har gjort hela världen till din granne
- Den elektroniska handeln förnyar affärs- och betalningsrörelserna.

Huvudsakliga källor till informationsläc
1. Samtal
2. Pappersdokument
3. Datasystem

Hanteringen kräver verktyg av olika slag

Utgångspunkten för hanteringen av informationsrisker är en identifiering av de viktigaste riskerna som är förknippade med information. På baksidan av denna broschyr finns en förteckning över informationsrisker. Förteckningen underlättar identifieringen av områden där de viktigaste informationsriskerna finns. Med hjälp av arbetskorten som ingår i verktygsserien kan man därefter genomföra en noggrannare identifiering och hantering. Vid hanteringen av risker bör de primära åtgärderna inriktas på en utveckling av verksamheten – verksamhetsmetoder, kunnande, ledning – och först därefter på tekniskt skydd.

Närmare information

- Informationssäkerhet, datasekretess, normer, instruktioner, stadgar, informationssäkerhetsreferenser. Ledningsgruppen för statsförvaltningens informationssäkerhet. http://www.vn.fi/vm/suomi/muuta/vahti/vahti.htm (Innehåller viktiga inhemska och utländska länkar)
- Informationssäkerhetsguide för smi-företag. Har du kontroll över företagets informationsrisker? Industrin och arbetsgivare. Finns även i pdf-format på adressen http://www.tt.fi/julkaisut/julkaisut.shtml

Författare: Matti Vuori, VTT Automaatio. Copyright © 2002 VTT. Verktygsserien har huvudsakligen finansierats av Europeiska socialfonden och social- och hälsoministeriets arbetarskyddsavdelning samt Arbetarskyddsfonden. Version 1.0. 29.4.2002 Fil: kor-tie-informationsrisker.doc. Översättning: Berg Translations.

Förteckning över informationsrisker

Företag:	Grupp/värderare:
Föremål för granskning:	Datum:

Ledning

- ☐ Ledningens medvetenhet om inf.riskernas betydelse
- ☐ Identifiering av den viktigaste informationen
- ☐ Identifiering av de största riskerna
- ☐ Informationspolitik och -praxis
- ☐ Datasäkerhet en del av kvalitetssystemet
- ☐ Tillräckligt kunnande
- ☐ Utveckling av informationssäkerhet

Verksamhets-utrymmen

- ☐ Benägenhet för olyckor
- ☐ Separering av företagets utrymmen i fastigheten
- ☐ Passerkontroll
- ☐ Bevakning inbrottssäkerhet
- ☐ Separering av utrymmen fr. varandra och passertillst.
- ☐ Hantering av arkiv och dokument
- ☐ Fax, skrivare, m.m.
- ☐ Kundutrymmen

Datasäkerhet

- ☐ Ansvar för systemen
- ☐ Hantering av dokument
- ☐ Användarrättigheter
- ☐ Distansarbete
- ☐ Verksamhetsuppföljning (störningar, användn., diskutr.)
- ☐ Arkiv och hantering av dokument
- ☐ Kontroll över förändringar
- ☐ Urbruktagning
- ☐ Programanskaffningar
- ☐ Kontroller
- ☐ Lösenord
- ☐ Extranet och WWW-sidor

Informations-risker

Personalens verksamhet

- ☐ Utbildning i hantering av informationsrisker
- ☐ Dataskyddsprinciper
- ☐ Klara verksamhetsanvisningar
- ☐ Verksamhet efter anställningen
- ☐ Kontroll av användarrättigheter
- ☐ Beredskap för störningar och olyckor
- ☐ Skyddande av personalens redskap (virusbekämpningsprogram m.m.)

Affärsrelationer

- ☐ Klassificering av samarbetspartner
- ☐ Gemensamma spelregler
- ☐ Risker beroende på underleverantörer
- ☐ Auditering av olika parter
- ☐ Avtal
- ☐ Systemanvändar-rättigheter
- ☐ Datasäkerhet i förhandlingsutrymmen m.m.
- ☐ Skydd av information mellan samarbetspartner gentemot övriga kunder

Ifyllningsexempel

☒ ~~Avtal~~ *Påtaglig risk;* OK Kunder *Under kontroll;* ☐ ~~Maskin-skador~~ *Gäller inte oss*

Ledning. Ledningens medvetenhet om informationsriskerna bildar basen för riskhanteringen. De praktiska verktygen består av ett kontrollerat informationsskydd, utnyttjande av kunnande och skapande av andra grundläggande möjligheter till riskhantering.

Personal. Informationsrisker hanteras inom ramen för personalens praktiska rutiner. Kunnande och planerade verksamhetssätt skapar basen för ett positivt resultat. Personalen bör ha tillgång till effektiva verktyg för kontrollen av risker, t.ex. automatiska virusbekämpningsprogram.

Utrymmen. Olyckor och stölder är vanliga risker. Passerkontroll, separering av utrymmen m.m. är viktiga åtgärder i hanteringen av informationsrisker.

Skydd av datasystem. Skydd av elektroniska datasystem är en utmaning inom hanteringen av informationsrisker. Men hanteringen av pappersbaserade system är precis lika viktigt.

Affärsrelationer. Informationsrisker i anslutning till affärsrelationer är aktuella i samband med nätbildning och underleveranser. Förutsättningarna för samarbete olika parter emellan bör utredas. Genom skolning och inspektering kan man se till att det inte förekommer svaga länkar i samarbetet. Förtroendet bör vara lika gott i varje riktning!